FACSIMILE COVER SHEET

Date: June 13, 2007

NUMBER OF PAGES INCLUDING THIS COVER SHEET: 18

TO	COMPANY NAME	FAX NUMBER
Mail Stop Appeal Brief - Patents	USPTO	571-273-8300

FROM: James F. Lea, III, Reg. No. 41,143

FELLERS, SNIDER, BLANKENSHIP, BAILEY & TIPPENS, P.C.
The Kennedy Building
321 South Boston Ave., Suite 800
Tulsa, Oklahoma 74103-3318
TELEPHONE: (918) 599-0621
TELECOPIER: (918) 583-9659

AUTO QUOTE: 57760

IF YOU DO NOT RECEIVE ALL OF THE PAGES OR IF ANY ARE ILLEGIBLE, PLEASE CONTACT US AT (918) 599-0621 AS SOON AS POSSIBLE.

MESSAGE: Attached, please find an Amended Appeal Brief for USSN 09/710,776.

****

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paper Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	1

Application Number	09/710,776
Filing Date	Nov 9, 2000
First Named Inventor	Candella, George J.
Art Unit	3621
Examiner Name	Pierre E. Elisca
Attorney Docket Number	57760/03-642

RECEIVED
CENTRAL FAX CENTER
JUN 13 2007

ENCLOSURES *(Check all that apply)*

- [ ] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment / Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance communication to (TC)
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please identify below):

Amended Appeal Brief

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	FELLERS, SNIDER, BLANKENSHIP, BAILEY & TIPPENS, P.C.		
Signature			
Printed name	James F. Lea, II		
Date	June 13, 2007	Reg. No.	41143

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature			
Typed or printed name	Stacy E. Jenkins	Date	June 13, 2007

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

RECEIVED
CENTRAL FAX CENTER

JUN 13 2007

PATENT
EXAMINING GROUP 3621

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): CANDELLA et al. Application No.: 09/710,776 Filed: 11/09/2000 Title: Method and System for Detecting Fraud in Non-Personal Transactions Art Unit: 3621 Examiner: Pierre E. Elisca Attorney Docket No.: FRA175/189535	CERTIFICATE OF MAILING UNDER 37 CFR 1.8 I hereby certify that this paper or fee is being deposited with the United States Postal Service with sufficient postage as "First Class Mail" and is addressed to Mail Stop Appeal Briefs-Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450, or is being transmitted via facsimile on this 13 day of June, 2007. Stacy Jenkins

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, Virginia 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPELLANT'S AMENDED APPEAL BRIEF

This Brief is in furtherance of the Notice of Non-Compliant Appeal Brief that was mailed in this case on June 5, 2007. The required fees, any required petition for extension of time for filing this Brief, and the authority and time limits established by the Notice of Appeal were dealt with in the TRANSMITTAL OF APPEAL BRIEF filed April 25, 2007.

This brief contains these items under the following headings, and in the order set forth below:

I. REAL PARTY IN INTEREST
II. RELATED APPEALS AND INTERFERENCES
III. STATUS OF CLAIMS
IV. STATUS OF AMENDMENTS
V. SUMMARY OF CLAIMED SUBJECT MATTER
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
VII. ARGUMENT
VIII. CLAIMS APPENDIX
IX. EVIDENCE APPENDIX
X. RELATED PROCEEDINGS APPENDIX

I. REAL PARTY IN INTEREST

The real party in interest in this Appeal is Fraud-Check.com, Inc., the assignee of record.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this Appeal. A previous Appeal Brief was filed for this case on July 12, 2004, but prosecution was reopened by the Office in response thereto. Subsequently, a Pre-Appeal Brief Request for Review was filed February 16, 2007. A Notice of Panel Decision from Pre-Appeal Brief Review, mailed April 2, 2007, instructed Applicants to proceed to the Board of Patent Appeals and Interferences.

III. STATUS OF CLAIMS

The status of the claims in this application is: Claims 1-32 are rejected. Claims 1-32 are being appealed.

IV. STATUS OF AMENDMENTS

No post-final amendments have been submitted.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claim	Subject Matter	Specification Reference		Drawing Reference	
1.	Method for detecting fraud in non-personal transactions comprising the steps of:				
	collecting **purchaser data** for the transaction,	Page	Line	Character	FIG.
		7	8, 12, 26	110	3
	said purchaser data comprising a **billing address**	Page	Line	Character	FIG.
		7	25, 26, 29	116	3
		8	21		
		9	29		
		10	2, 3		
		11	2, 4		

Claim	Subject Matter	Specification Reference		Drawing Reference	
	and a **ship-to address;**	Page	Line	Character	FIG.
		7	25	118	3
		8	1, 18, 25, 29		
		9	7, 23, 29, 30		
	transmitting said ship-to address to a **fraud-detection system;** processing said ship-to address to determine whether the transaction is potentially fraudulent by checking the purchaser's ship-to address against non-billing address criteria;	Page	Line	Character	FIG.
		6	13, 16, 28	100	2, 3
		7	5, 11, 23		
		8	4		
		17	16		
	and returning the relative risks of fraudulent activity associated with the transaction.				

The instant invention involves a method and system for detecting fraud in a non-personal transaction, e.g., a credit card purchase over the internet. The method and system include the steps of transmitting the purchaser's data, including a ship-to address for the transaction, to a fraud-detection system. The purchaser's data is then processed to determine whether the transaction is potentially fraudulent.

Notably, Applicant's method and system does not rely on billing address criteria, which is a distinguishing feature over the cited prior art and the subject of this appeal.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-32 are anticipated under 35 U.S.C. §102(e) by Walker et al. U.S. Patent No. 6,163,771.

VII. ARGUMENT

Applicant's method for fraud detection differs from the method cited by Walker because Applicant's method *does not utilize the billing address as a criteria to be checked against the shipping address*. Instead, the method and system may include any of the following steps: checking

to determine whether the purchaser's ship-to address exists; checking the purchaser's ship-to address against an historical database to determine whether a prior history of fraud exists, etc. (See pending application, p. 3, Summary of the Invention).

The basis for the Examiner's rejection is two-fold. First the Examiner asserts that Walker teaches a step of "processing said ship-to-address to determine whether the transaction is potentially fraudulent by checking the purchaser's ship-to-address against non-billing address criteria . . . (see., col 2, lines 7 – 20)"(Office Action of 11/16/2006, ¶5, p. 3). This rejection is relevant to claim 1. Second, the Examiner asserts that Applicant actually does utilize the billing address as criteria to be checked against the shipping address, citing claims 4, 6, 20 and 21 as proof (Office Action of 11/16/2006, ¶7b, p. 4). This rejection appears not relevant to claim 1. Both assertions are clearly erroneous, as set forth below. The practical significance of the billing address/ship-to address distinction was explained in the Amendment filed August 26, 2006[1].

First, the Examiner's assertions a) with respect to the teachings of Walker et al. will be examined, then b) the teachings and claim language of the pending Application will be examined.

a) With regard to Walker, the Examiner states, on pages 2 and 3 of the 11/16/06 Office

[1] "The Examiner's above example involving the dishonest waiter is illustrative in showing the inadequacy of existing methods of fraud detection and will, hopefully, provide the Applicant with an opportunity to more clearly explain the Applicant's invention. In the above example, which is elaborated upon, below, a dishonest waiter somehow obtains both a credit card account number and the cardholder's address. With this information, the dishonest waiter goes home and, e.g., orders a new stereo from an online electronics store. Presumably, the fact that the (cardholder's) billing address is different from the (dishonest waiter's home address) shipping address identifies the transaction as possibly suspicious.

A flaw in the above system is that the above suspicious transaction is indistinguishable from, reportedly, up to 30% of all legitimate transactions. As an example, it is common practice for an honest patent attorney to use his credit card to order products over the internet at the office during the lunch hour. The billing address of the credit card is the honest patent attorney's home address. However, since no one is at home during delivery hours, the honest patent attorney has the products shipped to his office, or perhaps ships a gift directly to a gift recipient. In this common scenario, the billing address and the shipping address are different, even though the transaction is completely legitimate. Thus, it can be seen that a "billing address different from shipping address" test flags so many legitimate transactions as potentially fraudulent that such a test is virtually worthless."

Applicant's method for fraud detection differs from the method cited by Walker and from the method described in the above two examples because Applicant's method *does not utilize the billing address as a criteria to be checked against the shipping address.* (Amendment filed 8/26/06, p. 13)

Action,

> Claims 1-32 have been rejected under the newly found prior Walker, Walker discloses a mail-order based credit card fraud, *both Visa and MasterCard have deployed databases that allow a merchant to verify that a given credit card account number is connected to a specific billing address*. Visa calls this service the Address verification service, the theory behind the service is that a thief (for example, a dishonest restaurant waiter) might be able to use a credit card receipt slip to steal an active account number, but if he tries to use that number for a mail order purchase he would not know the correct address associated with that number. Even if a thief were to obtain the cardholder's address, this service can allow a merchant to compare the shipping address of the catalog order to the current billing address for that account number and thus possibly identify any suspicious activity (which is readable as Applicant's claimed invention wherein said a method for detecting fraud non-personal transactions), comprising the steps of:
>
> Collecting purchaser data for the transaction, said purchaser data comprising *a billing address* and a ship-to-address; transmitting said ship-to-address to a fraud-detection system, processing said ship-to-address to determine whether the transaction is potentially fraudulent by checking the purchaser's ship-to-address against criteria, and returning the relative risk of fraudulent activity associated with the transaction (see, col 2, lines 7-20). (emphasis added)

Applicant's method for fraud detection differs from the method cited by Walker and from the method described in the above two examples because Applicant's method *does not utilize the billing address as a criteria to be checked against the shipping address*. (See Amendment filed 8/25/06, p. 13-15.)

The Examiner correctly reads Walker as requiring the use of billing address data. The Examiner directs Applicant to col. 2, lines 7 – 20. At col. 2, line16 -20, Walker states,

> "Even if a thief were to obtain the cardholder's address, this service can allow a merchant to compare the shipping address of the catalog order *to the current billing address* for that account number and thus possibly identify any suspicious activity."

The above teachings of Walker et al. flatly contradict the step required by the following claim element of claim 1:

> processing said ship-to address to determine whether the transaction is potentially fraudulent by checking the purchaser's ship-to address against <u>non-billing address</u> criteria;

b) With regard to the Examiner's assertion that Applicant actually does utilize the billing address, the Examiner states the following in paragraphs 7a and 7b on page 4 of the November 16, 2006 Office Action:

> a. Applicant's newly added limitation recites "checking the purchaser's ship-to address against non-billing address". Whereas, claim 6 recites ship-to address against the city and state with a Zip +4 code. Therefore, the ship-to address criteria can be billing address, a PO box address or any geographic area of the ship-to address.
>
> b. Applicant further argues that Applicant's method does not utilize the billing address as criteria to be checked against the shipping address. And yet, Claims 4, 6, 20 and 21 recite the purchaser's ship-to address criteria comprise comparing the city and state of the ship-to address against the city and state with a Zip + 4 Code. The city, the state, and the Zip + 4 code represent the person physical address, and can also be a billing address or a PO box address or an office address or a family member address. Accordingly, the specific billing address of Walker is the same as any regular address since they are used for the same purpose. Furthermore, an address is an address, it is just a label.

In response, Applicant wishes to point out that the city, the state, and the Zip + 4 code as used in the claims must be interpreted in the context of the claims. "The" city and state, as used in claims 4 and 6, clearly refer to the city and state and Zip + 4 code *of the ship-to address*. Further, claims 4 and 6 each depend from claim one, which unequivocally requires that the purchaser's ship-to address [be checked] against non-billing address criteria. Therefore, contrary to the Examiner's assertions, the city and state and Zip + 4 referred to in claims 4 and 6 is not just a label. Instead, the city, state and Zip + 4 comprises a criteria that is related to the ship-to address and is a criteria expressly defined as "non-billing address criteria".

With regard to claims 20 and 21, antecedent basis again requires that the zip code and the city and state with the ZIP + 4 code be interpreted as corresponding to the ship-to address.

As an example, Applicant's claim 6 states as follows:

> 6. (Previously Presented) The fraud detection method *according to claim 1*, wherein the step of checking the purchaser's ship-to address against criteria

> comprises comparing the city and state of the ship-to address against the city and state with a ZIP + 4 code. (emphasis added)

Claim 6 more narrowly defines the "step of checking the purchaser's ship-to-address against criteria...". The step of checking is set forth in base claim 1 as "... checking the purchaser's ship-to address against non-billing address criteria.

Claim 6 comprises, "comparing the city and state of the ship-to address against the city and state with a ZIP+4 code". This claim language is supported in Applicant's specification at page 8, lines 5 – 12 under the heading "Address Reasonableness and Existence Checking Step," which states as follows:

> The method and system for detecting fraud 100 is now able to process the purchaser's data to determine whether the transaction is potentially fraudulent. As shown in Figure 4, the address-checking procedure 122 receives the data in a usable format 131. An internal Post Office database is checked 132 to determine the existence of the address and the associated nine digit zip (i.e., ZIP+4). The use of the ZIP + 4 code permit appropriate identification of high fraud delivery points, since each nine ZIP + 4 code includes only a relatively small number of households (typically 400-500 households). If the system is unable to establish the existence of the ZIP + 4, a flag is set 134 to indicate this.

In summary, it can be seen that dependent claim 6 uses the city and state of the ship-to address and compares the city and state to the city and state with a ZIP+4 code, which is clearly non-billing address related, and further claim 6 depends from independent claim 1, which unambiguously defines the criteria to be checked as non-billing address criteria.

With regard to claims 20 and 21, antecedent basis again requires that the zip code and the city and state with the ZIP + 4 code be interpreted as corresponding to the ship-to address.

SUMMARY

For the reasons set forth above, Applicant submits that the Examiner's assertion that Walker teaches the step of checking the purchaser's ship to address against non-billing address criteria constitutes clear error. Applicant therefore requests allowance of the rejected claims.

Respectfully Submitted,

6-13-07
Date

James F. Lea III, Reg. No. 41,143
FELLERS, SNIDER, BLANKENSHIP,
BAILEY & TIPPENS, P.C.
321 South Boston, Suite 800
Tulsa, OK 74103-3318
(918) 599-0621
Attorneys for Applicant

Customer No. 22206
#405102 v1

CLAIMS APPENDIX

1. Method for detecting fraud in non-personal transactions comprising the steps of:

collecting purchaser data for the transaction, said purchaser data comprising a billing address and a ship-to address;

transmitting said ship-to address to a fraud-detection system;

processing said ship-to address to determine whether the transaction is potentially fraudulent by checking the purchaser's ship-to address against non-billing address criteria; and

returning the relative risks of fraudulent activity associated with the transaction.

2. The fraud detection method according to claim 1, wherein the processing step comprising parsing out the purchaser's ship-to address.

3. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises a step of checking to determine whether the purchaser's ship-to address exists.

4. The fraud detection according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises comparing a zip code of the ship-to address against a post office database.

5. The fraud detection method according to claim 4, wherein the zip code is a ZIP + 4 zip code.

6. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises comparing the city and state of the ship-to address against the city and state with a ZIP + 4 code.

7. The fraud detection method according to claim 1 wherein the step of checking the purchaser's ship-to address against criteria comprises the area code of the purchaser's phone number to determine whether it fits the geographic area of the ship-to address.

8. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises comparing the purchaser's ship-to address against the national change of address service database or the publisher's change of address database.

9. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises rating a building site associated with the "ship-to" address to determine whether the building or lot type is inconsistent with the transaction data.

10. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of checking the purchaser's ship-to address against an historical database to determine whether a prior history of fraud exists.

11. The fraud detection method according to claim 10, wherein the prior history of fraud determining step comprises checking whether a record associated with the purchaser's ship-to address exists in the historical fraud database.

12. The fraud detection method according to claim 11, wherein the associated record is checked to determine whether negative data is associated with the ship-to address.

13. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of checking the purchaser's ship-to address against an historical database to determine whether a pattern of fraudulent activity exists for the ship-to address.

14. The fraud detection method according to claim 13, wherein the pattern of fraud detecting step comprises determining whether an overlapping use of payment means and ship-to address is present by consulting a database of prior transactions.

15. The fraud detection method according to claim 13, wherein the pattern of fraud detecting step comprises retroactively notifying the merchant of previous transactions associated with the ship-to address once a pattern of fraudulent activity has been detected.

16. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of checking the purchaser's ship-to address against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends.

17. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of calculating a score based at least in part upon the likelihood that the transaction is fraudulent.

18. The fraud detection method according to claim 1, further comprising the step of checking to determine whether the purchaser's ship-to address exists.

19. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises comparing a zip code of the ship-to address against a post office database.

20. The fraud detection method according to claim 19, wherein the zip code is a ZIP + 4 zip code.

21. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises comparing the city and state of the ship-to address against the city and state with the ZIP + 4 code.

22. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises checking the area code of the purchaser's phone number to determine whether it fits the geographic area of the ship-to address.

23. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises comparing the purchaser's ship-to address against the national change of address service database or the publisher's change of address database.

24. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises rating the building site associated with the "ship-to" address to determine whether the building or lot type is inconsistent with the transaction data.

25. The fraud detection method according to claim 18, further comprising the step of checking the purchaser's ship-to address against an historical database to determine whether a prior history of fraud exists.

26. The fraud detection method according to claim 25, wherein the prior history of fraud determining step comprises checking whether a record associated with the purchaser's ship-to address exists in the historical fraud database.

27. The fraud detection method according to claim 26, wherein the associated record is checked to determine whether negative data is associated with the ship-to address.

28. The fraud detection method according to claim 25, further comprising the step of checking the purchaser's ship-to address against an historical database to determine whether a pattern of fraudulent activity exists for the ship-to address.

29. The fraud detection method according to claim 28, wherein the pattern of fraud detecting step comprises determining whether an overlapping use of payment means and ship-to address is present by consulting a database of prior transactions.

30. The fraud detection method according to claim 28, wherein the pattern of fraud detecting step comprises retroactively notifying the merchant of previous transactions associated with the ship-to address once a pattern of fraudulent activity has been detected.

31. The fraud detection method according to claim 28, further comprising the step of checking the purchaser's ship-to address against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends.

32. The fraud detection method according to claim 31, further comprising the step of calculating a score based at least in part upon the likelihood that the transaction is fraudulent.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.